



UNIVERSIDAD AUTONOM “TOMAS FRIAS”
INGENIERÍA DE SISTEMAS
(SIS-522)

ESTUDIANTE: Univ. Manuel Martinez Orcko **CI:** 8623998 **RU:** 110608

AUXILIAR: Univ. Aldrin Roger Perez Miranda

DOCENTE: Ing. Gustavo A. Puita Choque

PRÁCTICA 9

1) ¿Qué es el 'stack' en el contexto del lenguaje ensamblador y cómo se utiliza?

RESPUESTA

- Un 'stack' es una estructura de datos que funciona con el principio de LIFO.
- Se utiliza para almacenar información temporalmente durante la ejecución de un programa, como variables locales.
 - ◆ **PUSH:** Inserta un valor.
 - ◆ **POP:** Extrae el valor.
 - ◆ **CALL:** Llama a una subrutina, guardando la dirección de retorno en la pila.
 - ◆ **RET:** Retorna de una subrutina, recuperando la dirección de retorno de la pila.

2) Describe un escenario práctico donde el uso de ensamblador sería más ventajoso que el uso de un lenguaje de alto nivel

El uso de ensamblador sería más ventajoso en situaciones donde se requiere un control muy preciso sobre el hardware, como en el desarrollo de controladores de dispositivos, sistemas operativos, y software embebido para dispositivos de tiempo real o microcontroladores.

3) Explique cada línea del siguiente código del lenguaje ensamblador y diga qué es lo que se está haciendo

Línea 1: Mueve el valor 5 al registro AX.

Línea 2: Mueve el valor 10 al registro BX.

Línea 3: Suma el valor en BX al valor en AX.

Línea 4: Mueve el valor en AX al registro CX.

```
MOV AX, 5 ; Línea 1
MOV BX, 10 ; Línea 2
ADD AX, BX ; Línea 3
MOV CX, AX ; Línea 4
```

4) Explique detalladamente cómo funcionan los compiladores

Los compiladores son programas que traducen código fuente escrito en un lenguaje de alto nivel a un lenguaje de bajo nivel o lenguaje máquina que la computadora puede ejecutar directamente.

Paso 1: Convierte el código fuente en una serie de tokens, que son unidades básicas del lenguaje, como palabras clave, operadores, identificadores y literales.

Paso 3: Verifica la semántica del programa, asegurándose de que las operaciones sean válidas y significativas.

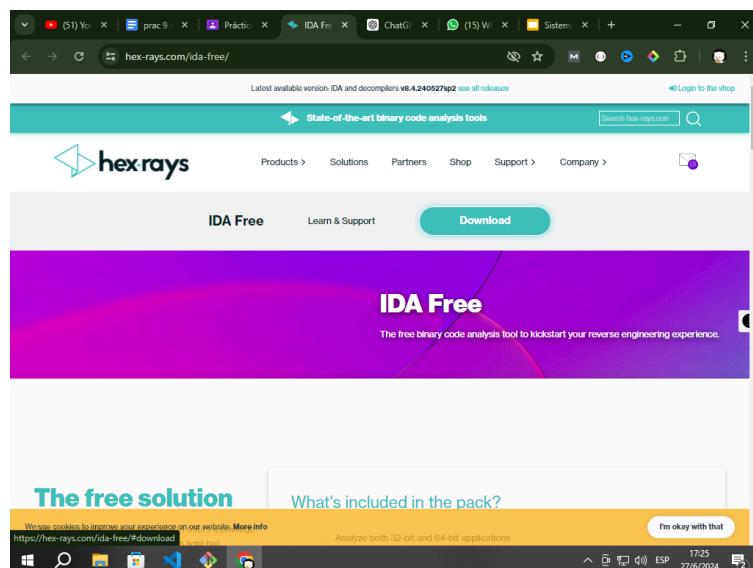
Paso 5: Convierte el código intermedio optimizado en código máquina específico para la arquitectura del procesador de destino.

Paso 2: Los tokens se organizan en una estructura que refleja la gramática del lenguaje, usualmente representada como un árbol de sintaxis	Paso 4: Mejora el código intermedio para hacerlo más eficiente, sin cambiar su comportamiento.	Paso 6: Traduce el código máquina a un archivo ejecutable y enlaza diferentes módulos del programa, incluyendo bibliotecas y funciones externas.
---	---	---

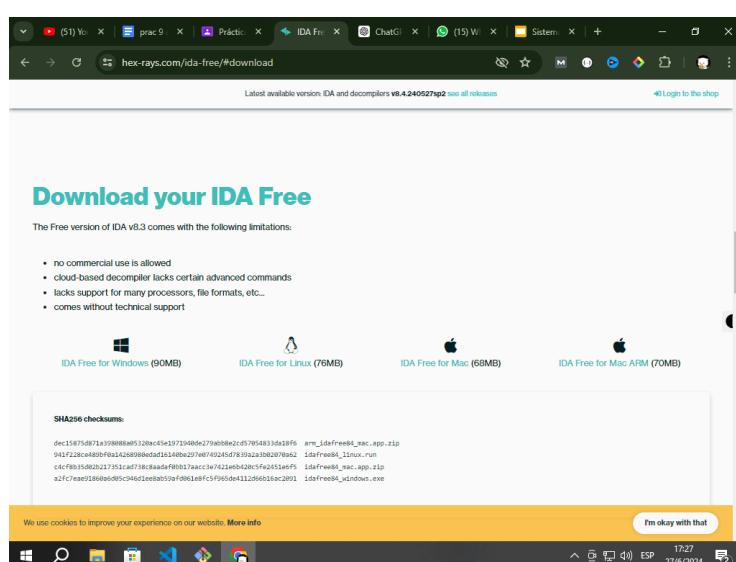
5) Realizar capturas de pantalla del siguiente procedimiento:

IDA: Es una de las herramientas más conocidas y potentes para el análisis de código binario y desensamblado. En este laboratorio se instalará IDA FREE pero también se tiene la versión de pago IDA PRO

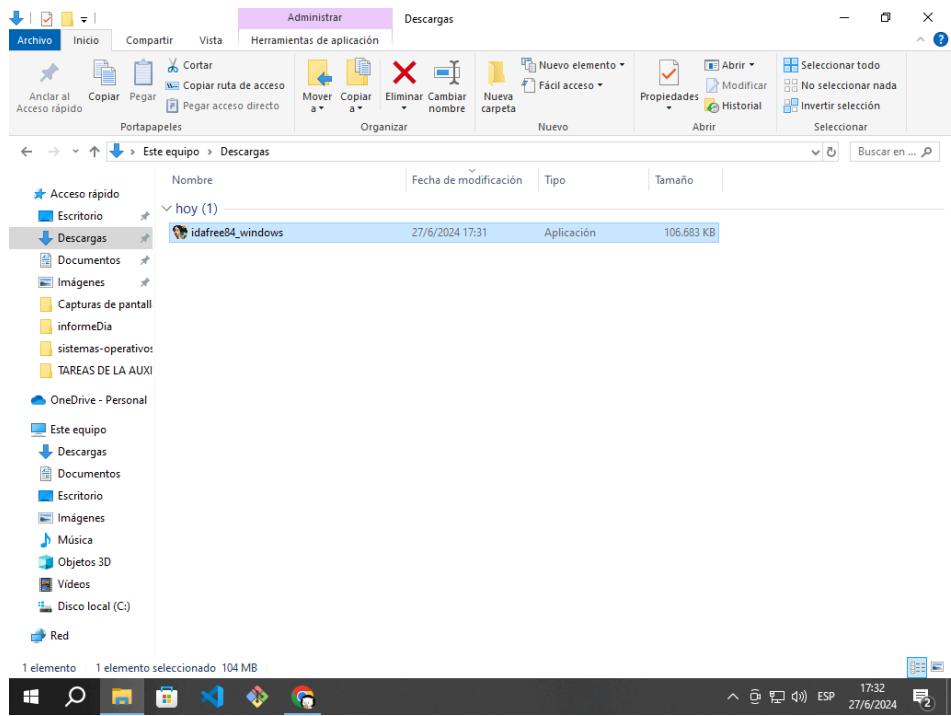
Paso 1: Descargar el software IDA FREE el cual lo podrá a hacer del siguiente enlace: <https://hex-rays.com/ida-free/>



[Ingresamos al enlace para descargar presionando en el botón de download].

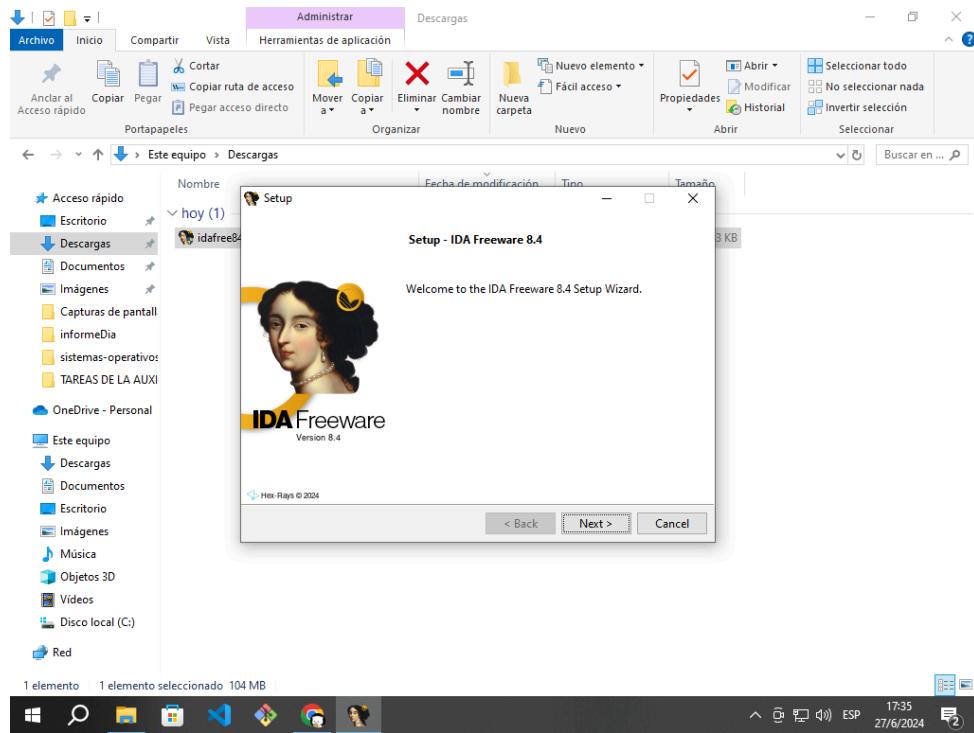


[Seleccionamos según el sistema operativo que se tiene]

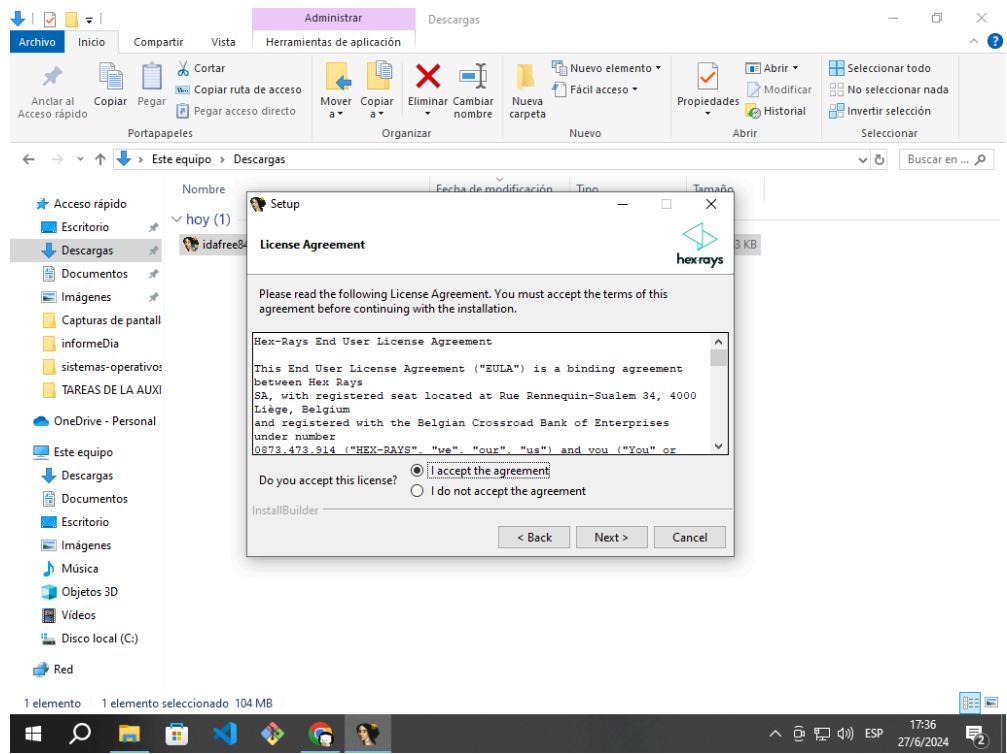


[Con eso ya tendríamos descargado el programa]

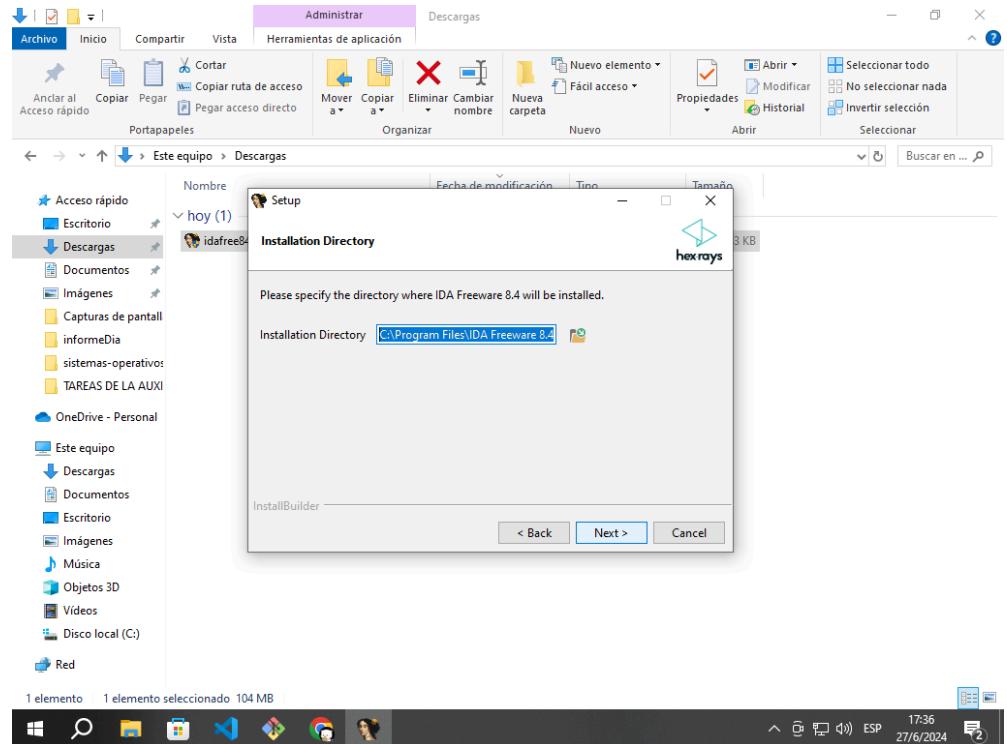
Paso 2: Instalación



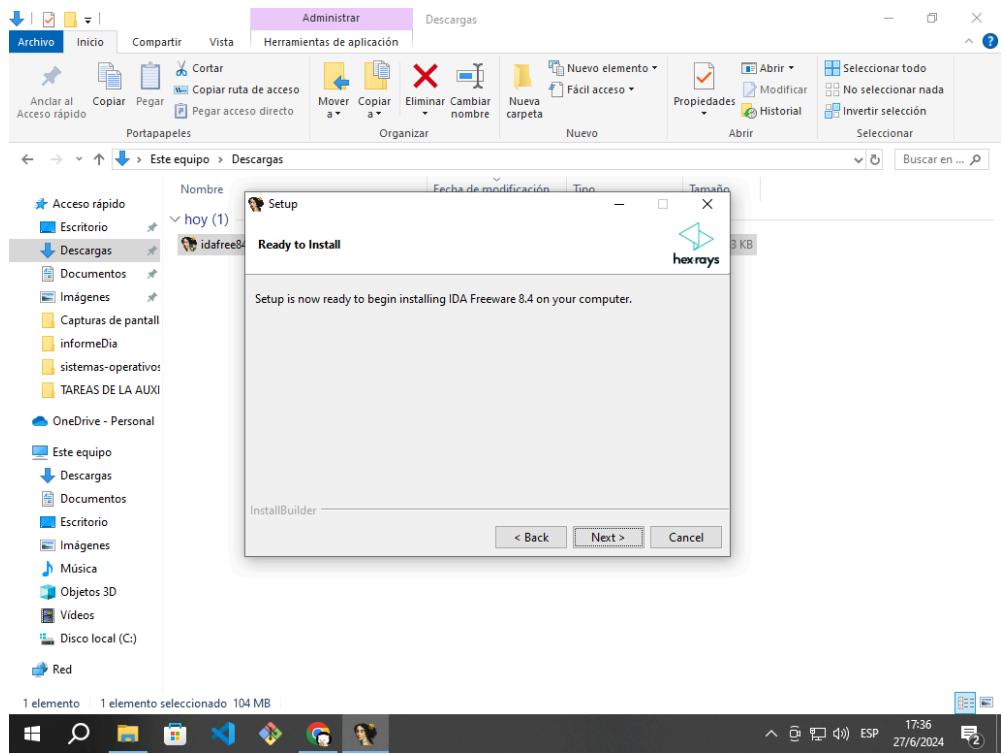
[Le damos a NEXT]



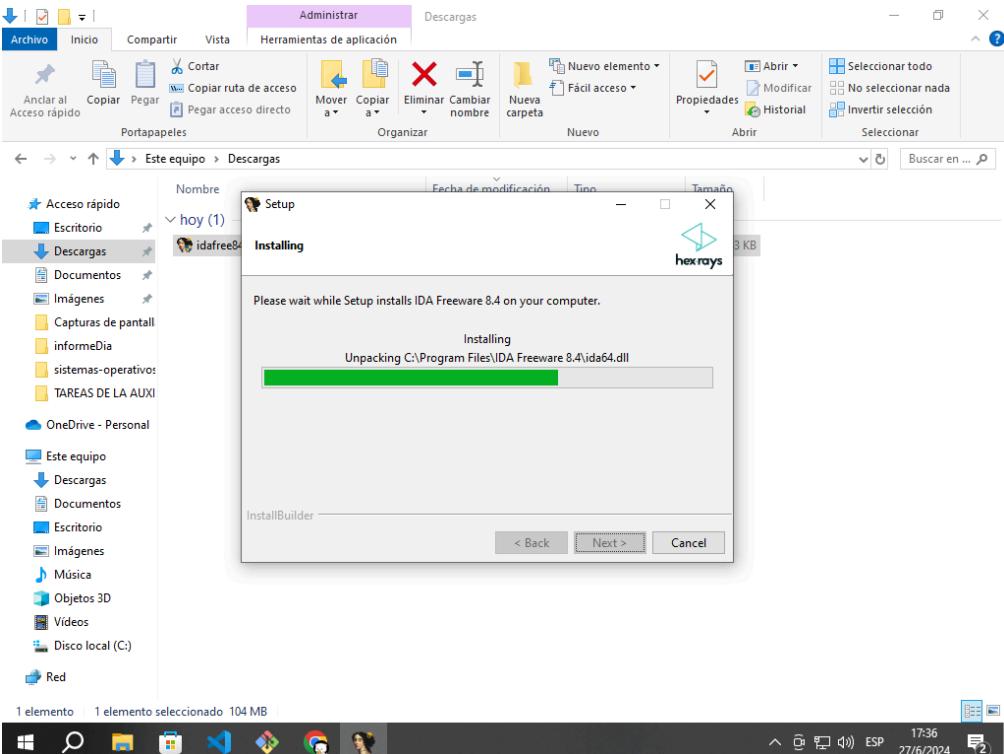
[Seleccionamos la primera opción y le damos a NEXT]



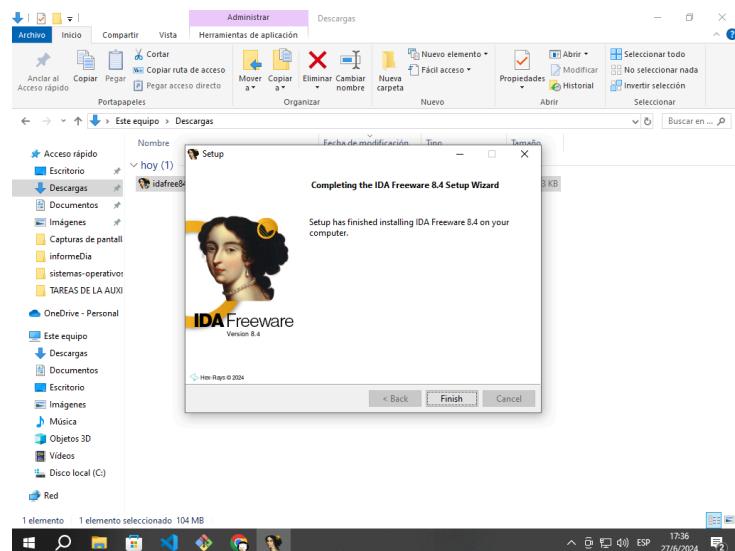
[Le damos a NEXT]



[Le damos a NEXT]



[Esperamos a que termine de cargar]



[Una vez finalizado le damos al botón de finalizar]

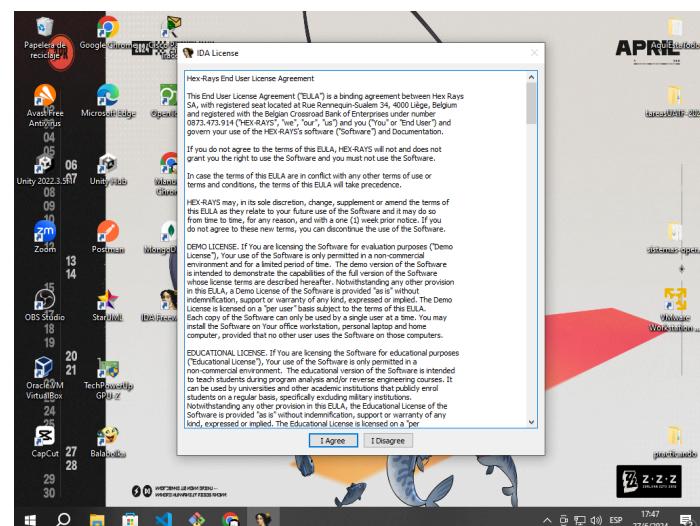


[Con eso ya tendríamos el programa instalado y ubicado en el escritorio]

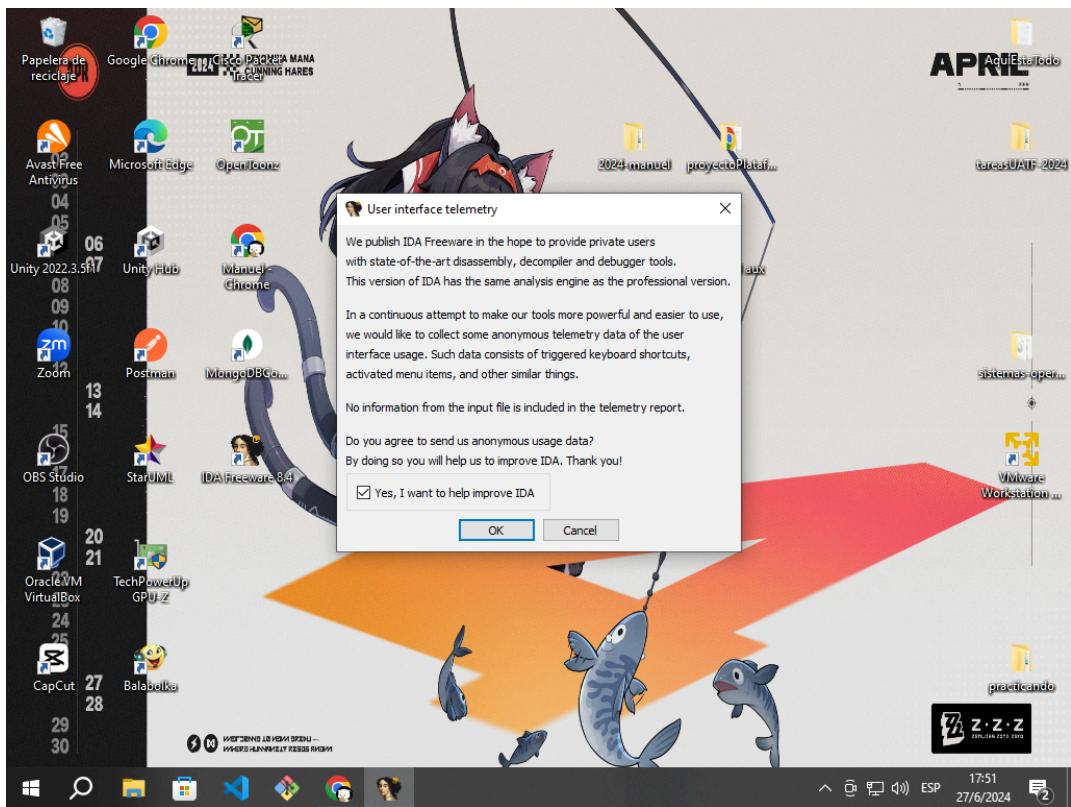
Paso 3: Procederemos a abrir un servicio en Windows



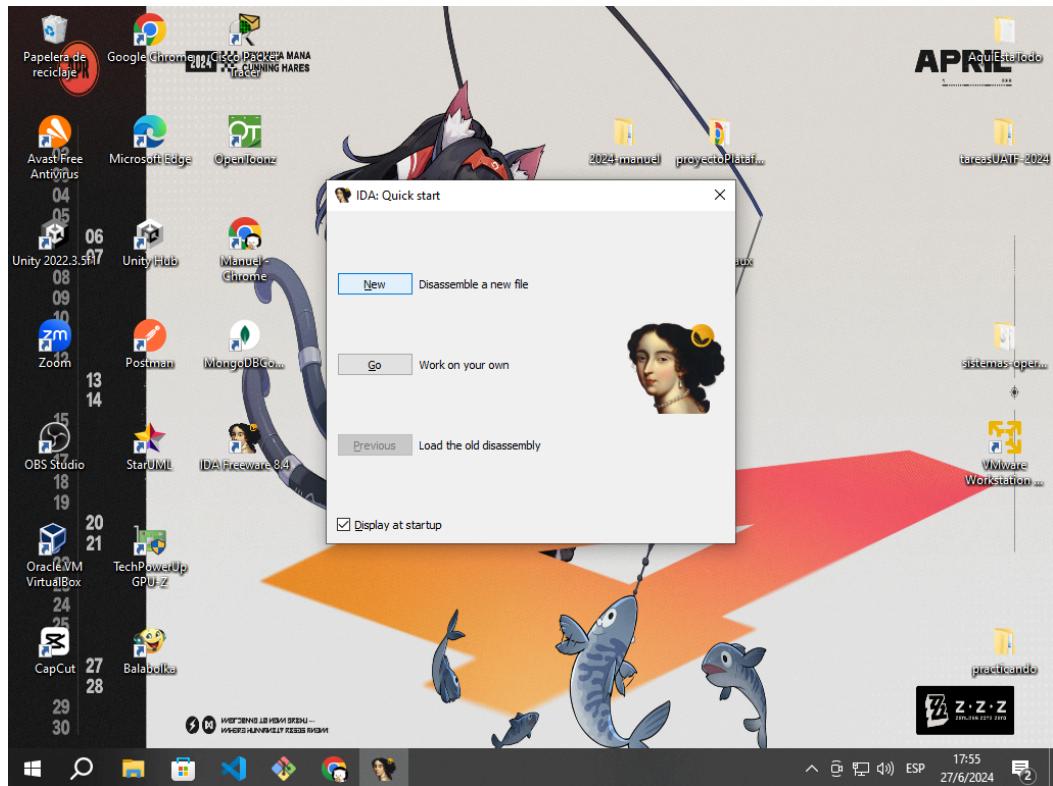
[Ejecutamos el programa]



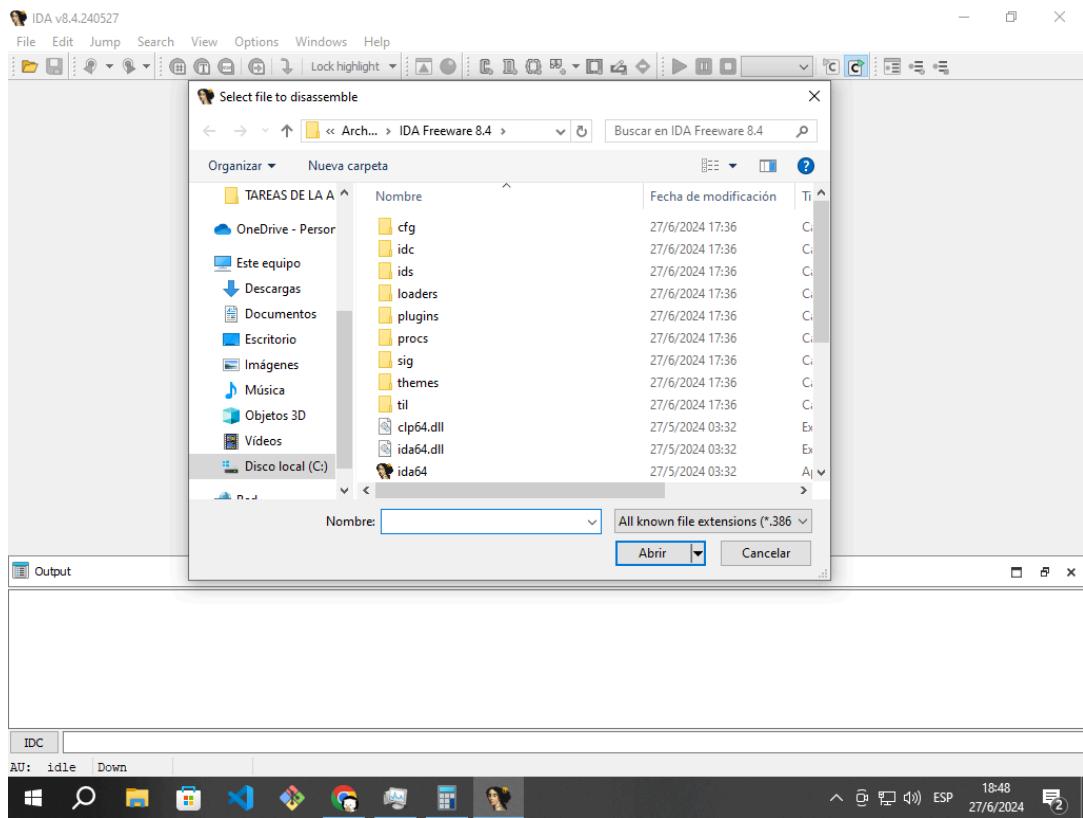
[Le damos a 'I Agree'(estoy de acuerdo)]



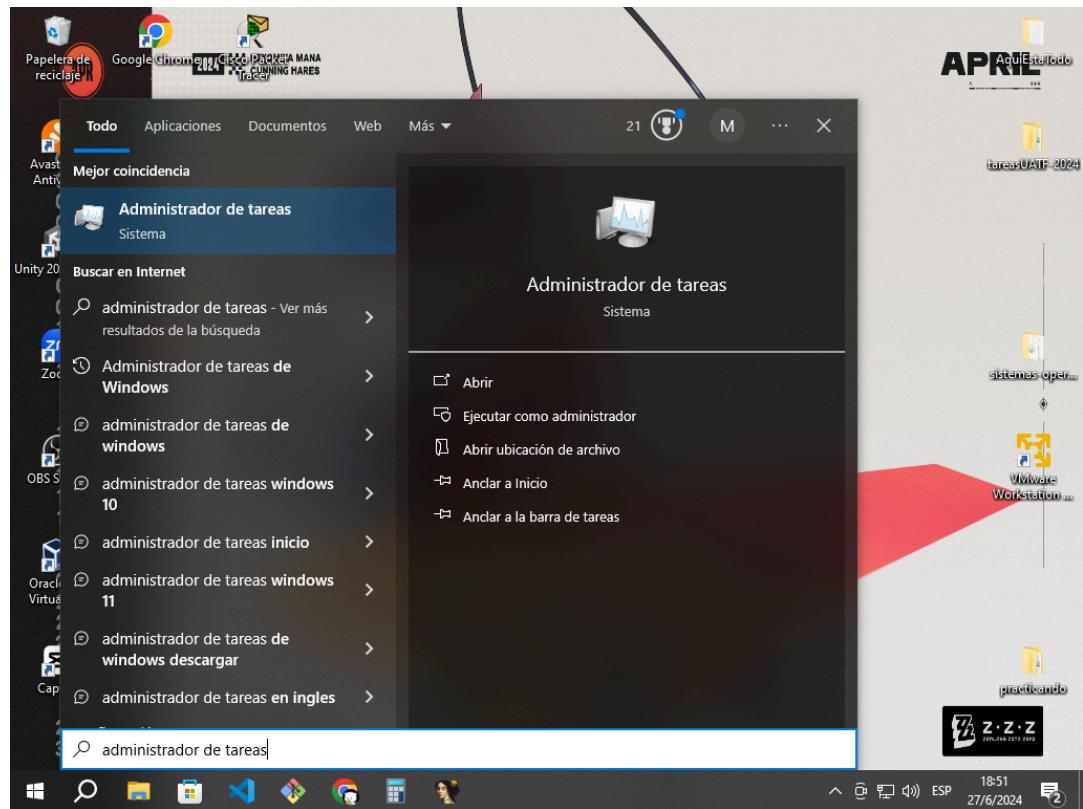
[Le damos a OK]



[Le damos en nuevo 'New']



[En este seleccionamos un servicio para analizar]



[Antes nos dirigimos al administrador de tareas]

Administrator de tareas

Archivo Opciones Vista

Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios

Nombre	Estado	0% CPU	51% Memoria	1% Disco	0% Red	Consumo de ...	Tendencia de ...
Aplicaciones (2)							
> Administrador de tareas		0%	21,5 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
> Google Chrome (13)		0%	596,0 MB	0 MB/s	0,1 Mbps	Muy baja	Muy baja
Procesos en segundo plano (62)							
AggregatorHost		0%	0,4 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Aislamiento de gráficos de disp...		0%	4,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
> Aplicación de subsistema de cola		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Application Frame Host		0%	6,6 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Avast Antivirus			1,5 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Avast Antivirus			14,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Avast Antivirus			0,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Avast Antivirus			2,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
> Avast Antivirus			6,0 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Avast Antivirus engine server			83,0 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
> Avast remediation exe			1,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Avast Service	0%	26,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja	
Avast Software Analyzer		0%	136,6 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Búsqueda		0%	0 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Calculadora (2)		0%	1,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja

Menos detalles Finalizar tarea

Windows 10 Task Manager screenshot showing the context menu for the Avast Service process. The 'Abrir ubicación del archivo' (Open file location) option is highlighted.

[Escogemos el servicio que queramos y abrimos en la ubicación del archivo]

Explorador de archivos

Administrador

Avast

Archivo Inicio Compartir Vista Herramientas de aplicación

Acceder rápido Copiar Pegar Mover Eliminar Cambiar nombre Nueva carpeta Fácil acceso Propiedades Abrir Seleccionar todo Modificar Historial Invertir selección

Portapapeles Organizar Nuevo

C:\Program Files\Avast Software\Avast

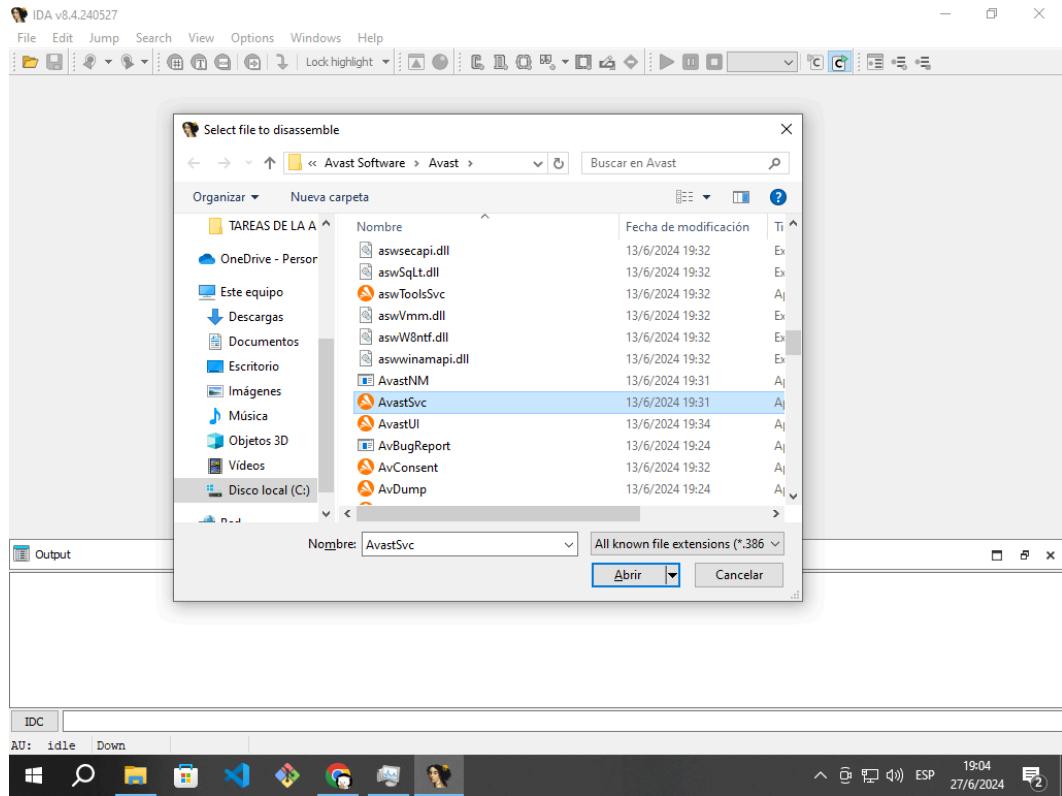
Nombre Fecha de modificación Tipo Tamaño

aswsecapi.dll	13/6/2024 19:32	Extensión de la ap...	1.819 KB
aswSql.dll	13/6/2024 19:32	Extensión de la ap...	1.019 KB
aswToolsSvc	13/6/2024 19:32	Aplicación	1.171 KB
aswVmm.dll	13/6/2024 19:32	Extensión de la ap...	260 KB
aswW0ntf.dll	13/6/2024 19:32	Extensión de la ap...	633 KB
aswwinamapi.dll	13/6/2024 19:32	Extensión de la ap...	122 KB
AvastNM	13/6/2024 19:31	Aplicación	2.305 KB
AvastNM	14/6/2024 19:04	Archivo de origen ...	1 KB
AvastNM_firefox	14/6/2024 19:04	Archivo de origen ...	1 KB
AvastSvc	13/6/2024 19:31	Aplicación	744 KB
AvastUI	13/6/2024 19:34	Aplicación	21.679 KB
AvastUI.exe.sum	13/6/2024 19:34	Archivo SUM	1 KB
AvBugReport	13/6/2024 19:24	Aplicación	4.777 KB
AvConsent	13/6/2024 19:32	Aplicación	727 KB
AvDump	13/6/2024 19:24	Aplicación	3.362 KB
AvEmUpdate	13/6/2024 19:31	Aplicación	4.961 KB
AvLaunch	13/6/2024 19:32	Aplicación	414 KB
BreachGuardSdk.dll	28/7/2023 13:28	Extensión de la ap...	2.050 KB
browser_pass.dll	13/6/2024 19:32	Extensión de la ap...	695 KB
burger_client.dll	13/6/2024 19:32	Extensión de la ap...	1.983 KB
chrome_100_percent.pak	28/7/2023 13:30	Archivo PAK	769 KB
chrome_200_percent.pak	28/7/2023 13:30	Archivo PAK	1.327 KB
chrome_elf.dll	6/1/2024 13:48	Extensión de la ap...	1.123 KB
CommChannel.dll	13/6/2024 19:31	Extensión de la ap...	1.598 KB

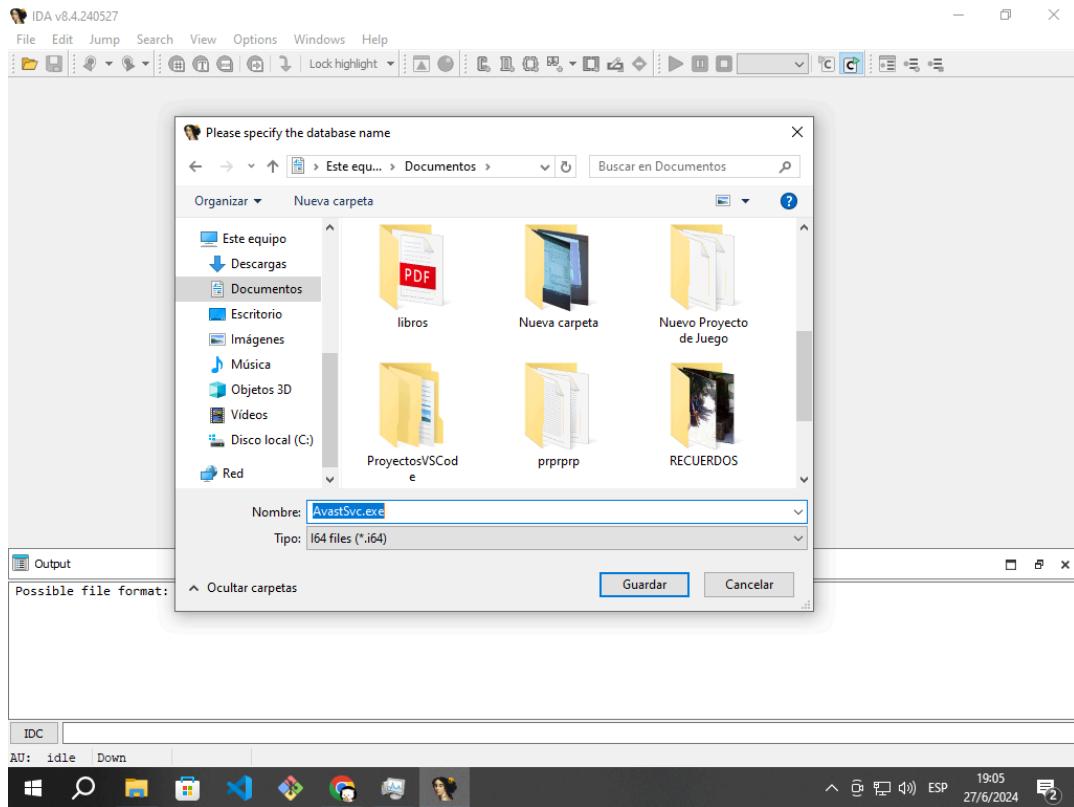
137 elementos 1 elemento seleccionado 743 KB

Windows 10 File Explorer screenshot showing the directory C:\Program Files\Avast Software\Avast. The AvastSvc executable is selected.

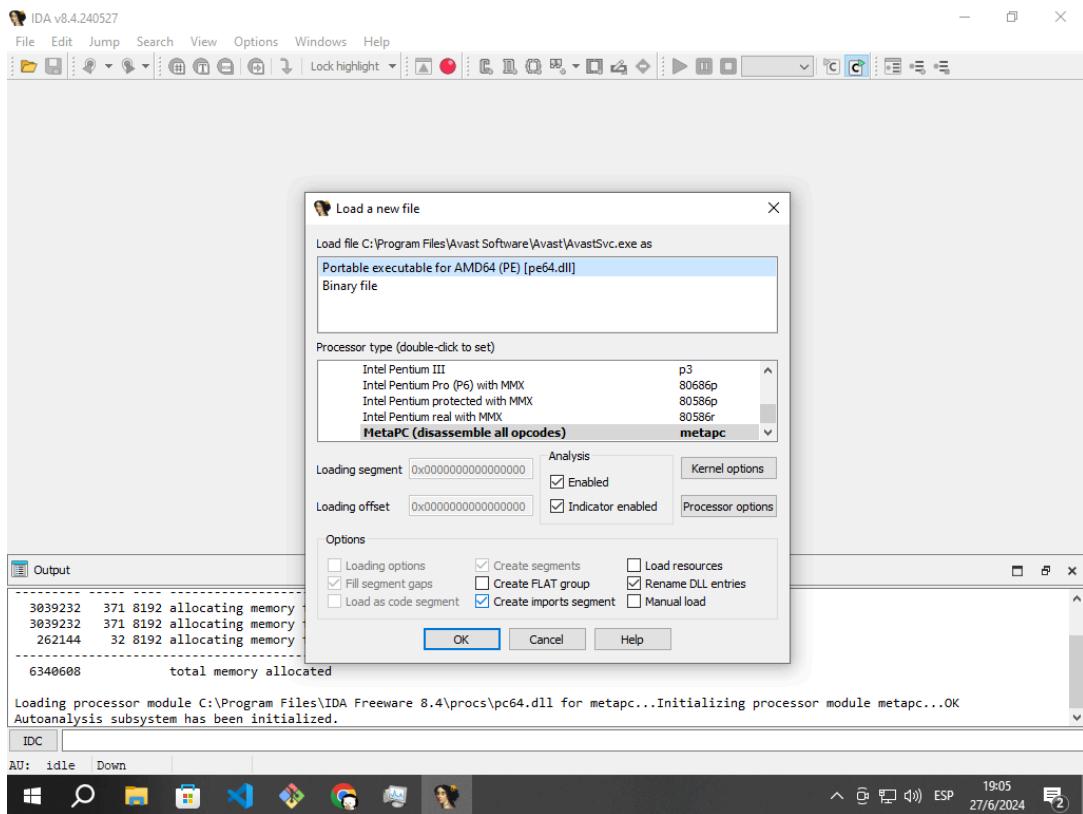
[Copiar el directorio del servicio]



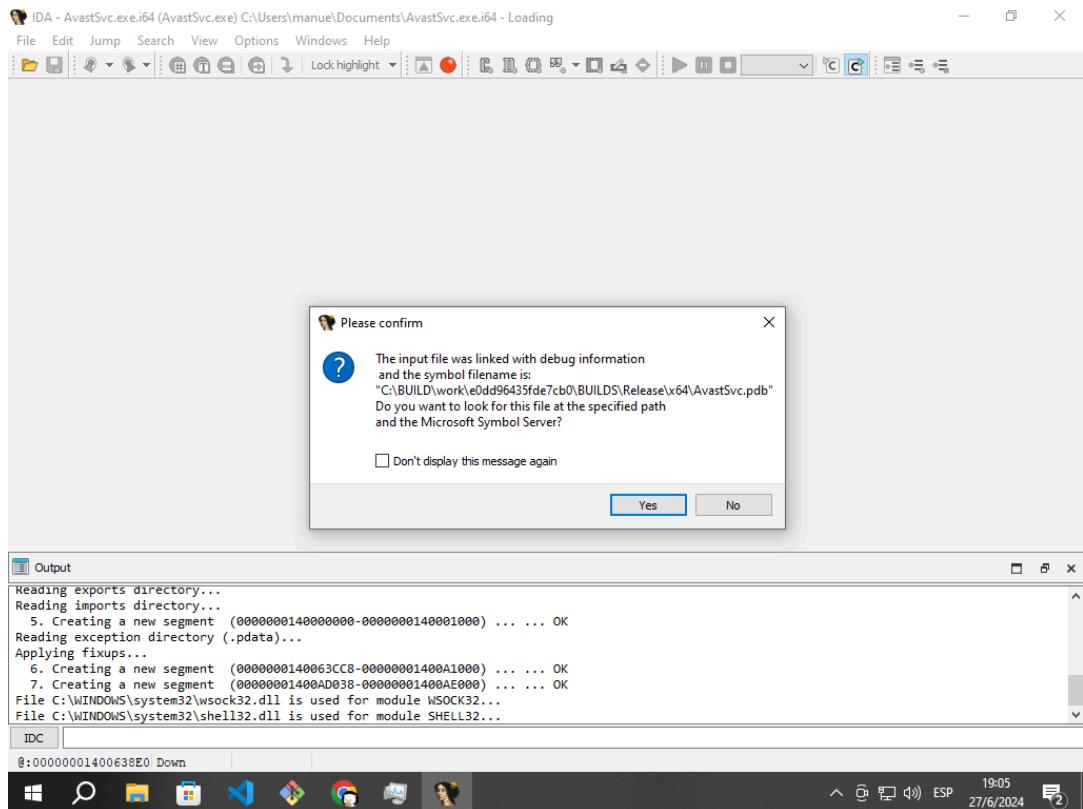
[Volvemos a la anterior ventana y introducimos el directorio que copiamos para luego escoger el servicio]



[Nos pedirá que guardemos]



[Una vez guardado se abrirá esta ventana y le damos a OK si tocar nada]



[En esta ventana se debe de presionar NO]

The screenshot shows the IDA Pro interface with the following details:

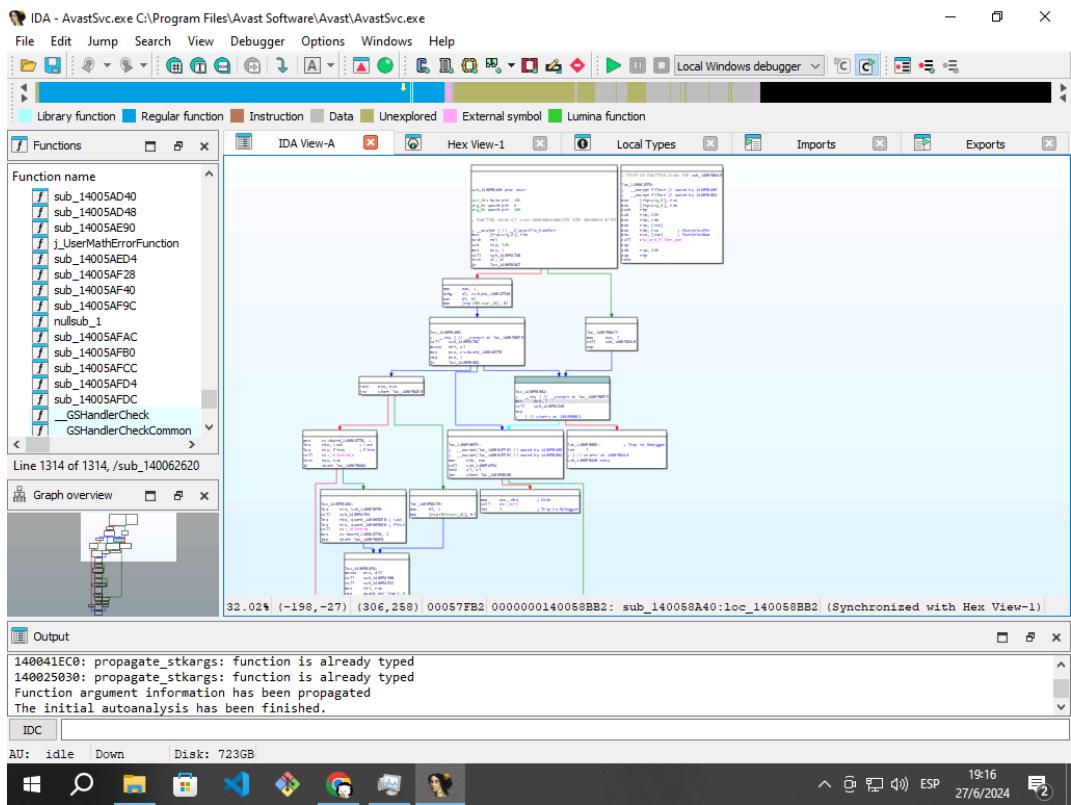
- Title Bar:** IDA - AvastSvc.exe C:\Program Files\Avast Software\Avast\AvastSvc.exe
- Menu Bar:** File, Edit, Jump, Search, View, Debugger, Options, Windows, Help
- Toolbar:** Includes icons for file operations, search, and debugger controls.
- Status Bar:** Local Windows debugger, 19:05, 27/6/2024
- Left Panel (Functions):** Shows a list of functions, many of which are subroutines starting with `sub_`. Some are highlighted in pink, such as `_C_specific_handler`, `_current_exception`, and `_current_exception_context`.
- Central Panel (IDA View-A):** Displays assembly code for the current function:

```
.text:00000001400588C0 ; [00000012 BYTES: COLLAPSED FUNCTION start. PRESS CTRL-NUMPAD0 TO EXPAND]
    .text:00000001400588D2 align 20h
    .text:00000001400588E0
    .text:00000001400588E0 ; ====== S U B R O U T I N E ======
    .text:00000001400588E0
    .text:00000001400588E0
    .text:00000001400588E0
    .text:00000001400588E0
    .text:00000001400588E0 sub_140058BE0 proc near ; CODE XREF: sub_140061F10+164p
    .text:00000001400588E0 mov    [rsp+10h], rbx
    .text:00000001400588E5 mov    [rsp+8], rcx
    .text:00000001400588E5 push   rdi
    .text:00000001400588E6 sub    rsp, 20h
    .text:00000001400588E7 mov    rdi, [rsp+30h]
    .text:00000001400588E8 lea    rdx, ASwMainImpl@E ; asw::main::impl::at_exit_acti...
    .text:00000001400588E9 mov    rcx, rdi
    .text:00000001400588EA call   sub_140058E0A
    .text:00000001400588C0 lea    rax, off_1400E150
    .text:00000001400588C0 mov    [rdi], rax
    .text:00000001400588C0 lea    rcx, [rdi+28h]
    .text:00000001400588C1 xor    eax, eax
    .text:00000001400588C1 mov    [rdi+30h], rax
    .text:00000001400588C17 call   cs:_ExceptionPtrCreate@@YAXPEAX@Z ; __ExceptionPtrC...
    .text:00000001400588C18 lea    rcx, [rdi+28h]
    .text:00000001400588C21 call   cs:_ExceptionPtrCurrentException@@YAXPEAX@Z ; __Exc...
    .text:00000001400588C25 mov    rbx, [rsp+38h]
    .text:00000001400588C28 mov    rax, rdi
    .text:00000001400588C30 add    rsp, 20h
    .text:00000001400588C33
Line 1472 of 1472, /sub_140062620
```
- Bottom Panel (Output):** Displays the message: "Hex-Rays Decompiler plugin has been loaded (v8.4.0.240527) License: 48-F4EE-0000-00 Freeware version (1 user) The decompilation hotkey is F5. Please check the Edit/Plugins menu for more information."
- Bottom Left:** IDC button
- Bottom Right:** Disk status: Disk: 722GB

[Con todo esto deberías ver algo similar a la imagen]

Paso 4: Finalmente, se podrá ver código Assembler del servicio que hemos desensamblado

[Ahora se puede observar código Assembler]



[También podemos ver la estructura de tablas]